ABSTRACT OF THE INVENTION

Disclosed is an authentication mechanism that enables an information recipient to ascertain that the information comes from the sender it purports to be from. This mechanism integrates a private/public key pair with selection by the sender of a portion of its address. The sender derives its address from its public key, for example, by using a hash of the key. The recipient verifies the association between the address and the sender's private key. The recipient may retrieve the key from an insecure resource and know that it has the correct key because only that key can produce the sender's address in the message. The hash may be made larger than the sender-selectable portion of the address. The recipient may cache public key/address pairs and use the cache to detect brute force attacks and to survive denial of service attacks. The mechanism may be used to optimize security negotiation algorithms.